What is claimed is:

1. A memory device comprising:

a first tamper resistant memory which cannot be accessed directly by an electronic device; and

a second non-tamper resistant memory which cannot be directly accessed by the electronic device,

wherein data stored in the first memory is saved to the second memory.

2. The memory device according to claim 1,

wherein the saved data is data prepared when installing an application program or executing the application program.

3. The memory device according to claim 2,

wherein when the data is saved to the second memory, the program code of the application program is rejected from the first memory.

4. The memory device according to claim 2,

wherein when the data is saved to the second memory, the program code of the application program is left in the first memory.

5. The memory device according to claim 1,

wherein the saved data includes the data prepared

when installing the application program or executing the application program and the program code of the application program.

6. The memory device according to claim 1, further comprising:

a managing table in which the managing information for the data stored in the first memory is described,

wherein the managing information includes information indicating whether or not the data can be saved.

7. The memory device according to claim 2,

wherein the application program is downloaded in the first memory and installed in the first memory.

8. The memory device according to claim 2,

wherein the application program is downloaded in the second memory and installed in the first memory.

9. The memory device according to claim 2,

wherein the application program is downloaded in the second memory and installed in the second memory.

10. The memory device according to claim 1,

wherein the saved data and the signature

information for the data are encoded and saved to the second memory.

11. The memory device according to claim 1,

wherein the first memory includes a saved information managing unit for managing saved information, data to be saved is encoded and saved, and the signature information of the encoded data is stored in the saved information managing unit.

12. The memory device according to claim 1,

wherein data to be saved is determined on the basis of an instruction from an electronic device.

13. The memory device according to claim 1,

wherein if there is no space area for downloading or installing data in the first memory when an instruction to download or install the application program in the first memory is received, arbitrary data which is accumulated in the first memory and possible to be saved is saved to the second memory

14. The memory device according to claim 1,

wherein specific saved data is restored in accordance with a restoration instruction from the electronic device.

15. The memory device according to claim 1,

wherein the saved data related to the application program is restored in accordance with a start instruction of the application program from the electronic device.

16. A memory device comprising:

a tamper resistant module including an inner CPU and a first memory, to which external devices can not directly access;

a non-tamper resistant memory including a second memory, to which external devices can not directly access;

a control part for controlling access to the tamper resistant module and the non-tamper resistant memory from external devices;

wherein said inner CPU is capable of directly accessing to both the first memory and the second memory, detects space areas of both the first memory and the second memory, and instructs to exchange necessary data to execute an application program between the first memory and the second memory in accordance with the detected space areas and/or command from an external device authenticated by the control part.